VIRDI 4000 - Guia do Usuário

Versão PT-1.00

< **Terminologia** >

Admin, Administrador

- O administrador é o usuário que tem acesso ao Menu de configurações do terminal, que pode cadastrar/modificar/apagar usuários e mudar as configurações do terminal.
- Caso não tenha nenhum administrador cadastrado, qualquer pessoa pode acessar o menu do terminal e mudar alguma configuração. Portanto, é extremamente recomendado que se tenha pelo menos um administrador cadastrado.
- O administrador tem permissão para mudar configurações importantes. Atenção ao fazer alguma modificação no cadastro e operação.

Identificação 1:1 (Verificação 1:1)

- Refere-se ao método no qual a digital inserida é comparada com a digital cadastrada no ID do usuário ou no Cartão.
- Esse método é chamado de Identificação 1:1 porque a digital é comparada somente com a digital cadastrada no banco de dados referenciada pelo ID ou no Cartão RFID do usuário.

Identificação 1 para N

Refere-se ao método no qual a digital inserida é comparada com o banco de dados do terminal, sem que haja uma referência da digital com o ID ou cartão RFID do usuário.

I-Capture (Captura Inteligente)

Reforça a capacidade de detecção contra marcas de digitais residuais (marcas de digitais que ficam no sensor biométrico, devido a suor ou resíduos no dedo) e automaticamente ajusta as configurações do sensor para ler as digitais com boas qualidades, independente das condições da pele (seca ou molhada).

Nível de Autenticação

É um nível de segurança de autenticação, tem escala de 1 a 9 de acordo com o grau de concordância. A autenticação vai ser sucedida quando o grau de concordância entre duas digitais comparadas for maior que o nível de autenticação estabelecido.
Quanto maior o nível de autenticação, maior será o nível de segurança. Porém, requer maior taxa de concordância, então a probabilidade de ocorrer falha na autenticação pode aumentar.
- Nível 1:1 de autenticação é usado para Identificação 1:1
- Nível 1:N de autenticação é usado para Identificação 1:N

Método de autenticação

Os métodos de autenticação podem ser: autenticação biométrica (FP), autenticação por cartão (RF), por senha e várias formas de autenticação a partir da combinação destes métodos.
Exemplo: Autenticação por Cartão ou Biometria se refere quando a autenticação for feita usando a biometria ou o cartão, um dos dois.

Teclas de Função

- Estão disponíveis as seguintes teclas: [F1], [F2], [F3], [F4], [ENTER]. Essas teclas são usadas para fazer autenticação e cada tecla representa um modo de autenticação.

Índice

1. Cuidados especiais durante o uso

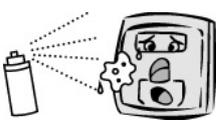
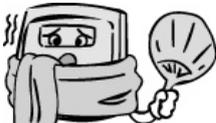
Cuidados e Avisos de Segurança

- **Atenção**

Não opere o dispositivo com mãos molhadas e não deixe cair líquido no dispositivo. ->Pode quebrar ou causar choque elétrico.	Não aproxime objetos que causem fogo perto do terminal. ->Pode causar incêndio.
Não desmonte, abra ou modifique o dispositivo. -> Podem quebrar, causar choque elétrico ou incêndio.	Mantenha o terminal fora do alcance de crianças. ->Pode quebrar o terminal ou causar acidentes com crianças.

- Se os itens não forem seguidos devidamente, pode causar sérios prejuízos a saúde ou até mesmo morte.

- **Precauções**

Não exponha diretamente a luz do sol. ->Pode ocorrer deforma-ção ou descoloração.	Não coloque em lugares com muita umidade ou poeira. ->Pode danificar.
Não borrife água para fazer a limpeza do terminal. Não use benzeno, tíner ou álcool para limpeza. ->Pode causar choque elétrico ou incêndio.	Não aproxime materiais magnéticos. ->Podem quebrar ou causar mau funciona-mento do terminal.
Não suje a área do sensor biométrico. ->As digitais podem não ser reconhecidas devidamente.	Não borrife pesticidas ou líquidos inflamáveis no terminal. -> Podem ocorrer defor-mação ou descoloração.
Dispositivo não resistente a impactos. Não encoste objetos pontiagudos. -> Pode danificar.	Não instale em lugares com grandes variações de temperatura. -> Pode danificar.

- Se os itens não forem seguidos devidamente, podem ocorrer danos e prejuízos.

Não nos responsabilizamos por acidentes ou estragos causados se as recomendações não forem seguidas.

2. Introdução

2.1. Recursos

- **Sistema de Controle de Acesso usando a rede (LAN)**
  - Como a comunicação entre o leitor biométrico e o servidor de autenticação é feito usando cabo UTP e protocolo TCP/IP, pode ser usada a instalação da rede local existente. A auto-detecção da rede 10/110Mbps fornece rápida velocidade e permite fácil gerenciamento e monitoração através da rede.

- **Função de auto detecção conveniente**
  - A operação de autenticação requer somente a impressão digital sem necessitar inserir uma chave adicional.

- **Simples autenticação usando biometria**
  - O uso da tecnologia de identificação biométrica previne contra perda de senha, cartão, chave ou roubo. Como é usada a biometria, o nível de segurança da autenticação é aumentado significativamente.

- **Mensagens de orientação de uso no LCD e por voz**
  - Através de mensagens da tela de LCD e de voz, toda autenticação é processada com mensagens de orientação. A luz de fundo da tela de LCD permite fácil visualização mesmo em ambientes escuros. Como a voz é salva na memória, é possível fazer a mudança de voz para outro idioma através do servidor.

- **Vários e flexíveis métodos de controle de acesso**
  - Uso conveniente e previne contra empréstimo, falsificação e perda de cartão ou chave.
  - Perfeita função de controle de acesso garantindo diferenciação de acesso para cada grupo de usuário.
  - Flexibilidade no controle de acesso podendo limitar o horário de acesso.
  - Baixo custo de manutenção e de desenvolvimento comparado a outros dispositivos de controle de acesso.
  - Não há a necessidade em ter que emitir um cartão de visita para visitantes.

- **Usado em aplicações para vários tipos de sistemas, como controle de acesso, controle de ponto e controle de refeições.**
  - Várias aplicações diferentes disponíveis. O método de operação pode ser configurado no menu do terminal.

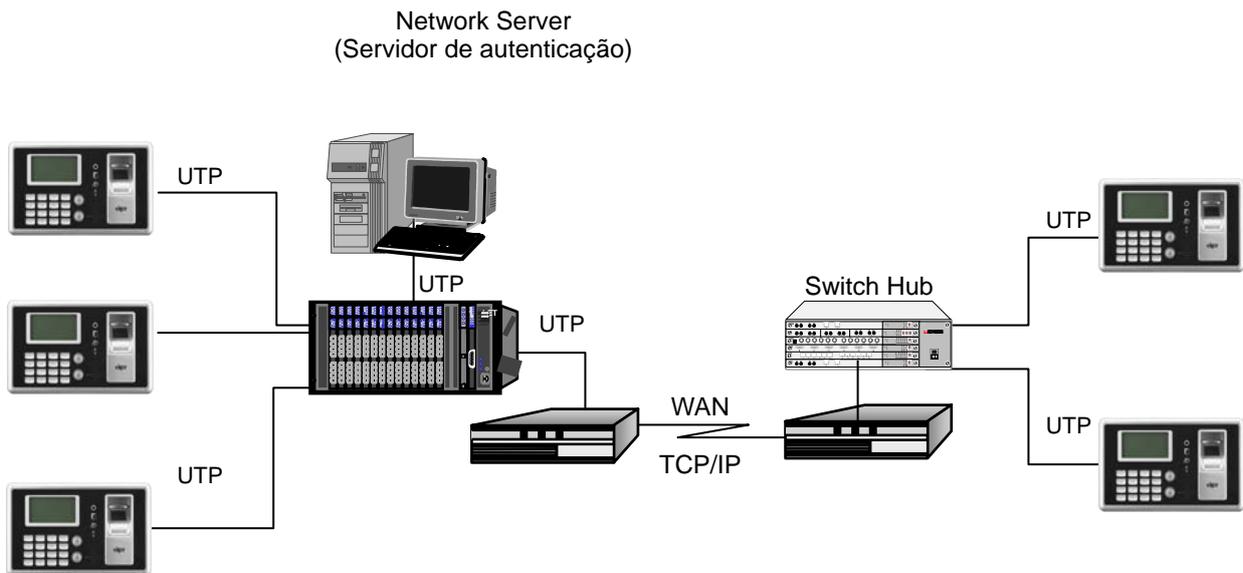
- **Alta capacidade de armazenamento do terminal e servidor**
  - Não há limitações de usuários para cadastro no servidor e o terminal pode armazenar até 3000 usuários.

- **Interfone**
  - Interface para conectar um interfone ao terminal, permitindo fácil identificação do visitante.

- **Vários métodos de cadastro e autenticação**
  Existem 11 métodos de cadastro e autenticação disponíveis para usuários. Que devem ser escolhidos antes de fazer o cadastro do usuário ou do administrador.

Método	Descrição
FP	Cadastro da digital Autenticação pela digital
ID&PW	Cadastro de senha Autenticação digitando o ID seguido pela senha
FP|PW	Cadastro de senha e digital Autenticação por senha ou digital
FP&PW	Cadastro de senha e digital Autenticação por digital seguido pela senha
RF	Cadastro do cartão Autenticação pelo cartão
RF|FP	Cadastro do cartão e digital Autenticação pelo cartão ou digital
RF&FP	Cadastro do cartão e digital Autenticação pelo cartão seguido pela digital
RF|PW	Cadastro de cartão e senha Autenticação por cartão ou senha
RF&PW	Cadastro de cartão e senha Autenticação por cartão e senha
ID&FP|RF&FP	Cadastro de cartão e digital Autenticação digitando o ID seguido pela digital ou autenticação por cartão e seguido pela digital
ID&PW|RF&PW	Cadastro de cartão e senha Autenticação digitando o ID seguido pela senha ou autenticação por cartão seguido pela senha

3. Configuração do Sistema

3.1 - Configuração em rede

3.2 - Configuração standalone

4. Partes do Terminal

Microfone

LED: status da operação

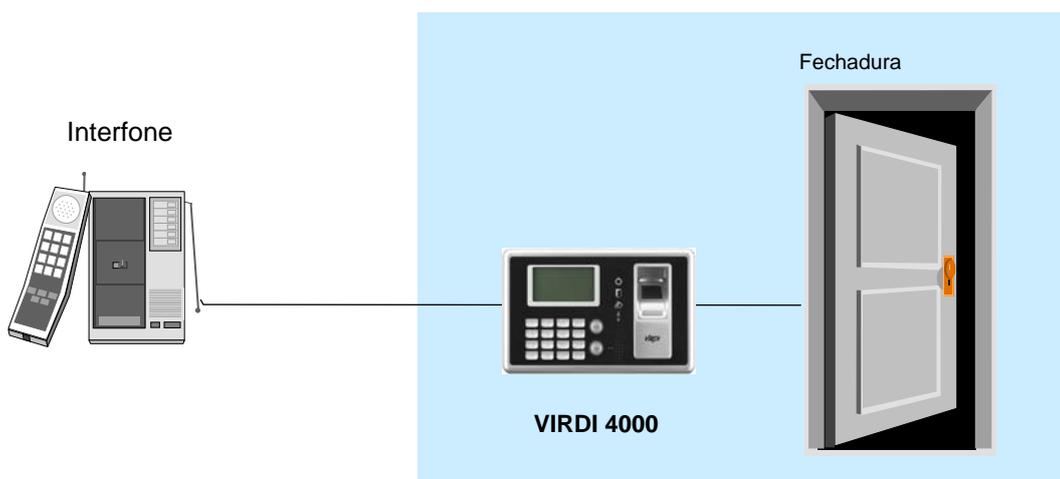
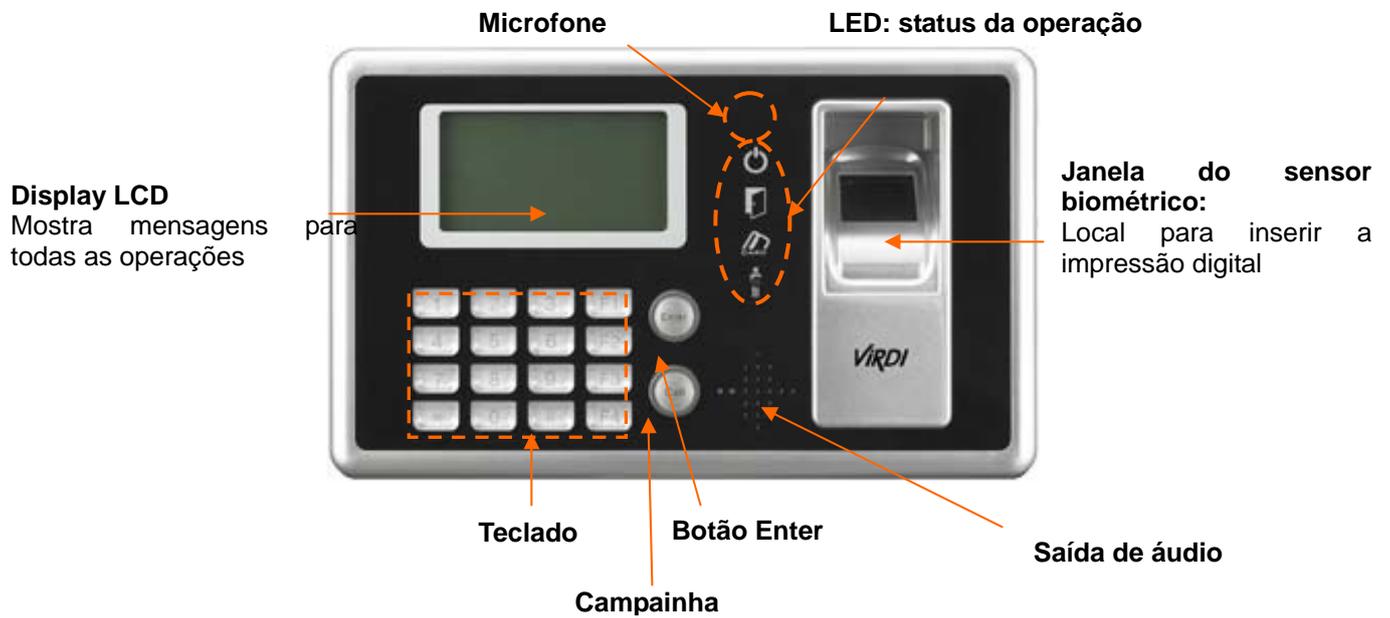
Display LCD
Mostra mensagens para todas as operações

Janela do sensor biométrico:
Local para inserir a impressão digital

Teclado

Botão Enter

Saída de áudio

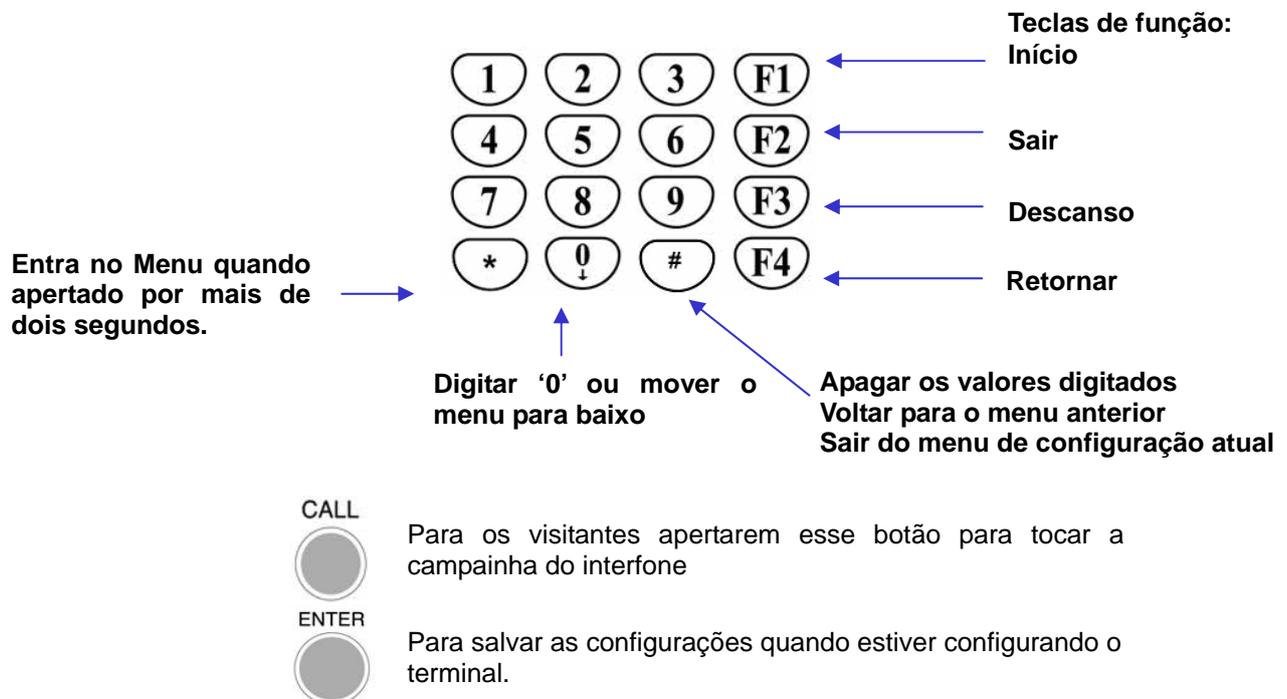
Campainha

5. Especificações

Item	Especificação	Nota
CPU	32-Bit RISC CPU (266MHz)	
Memória	32M SDRAM	
	32M FLASH (Padrão)	20.240 digitais
Sensor biométrico	Óptico	
Tempo de authentic.	<1 seg.	
Área scanner/ Resolução	12,9 x 15,2mm / 500 DPI	
FRR / FAR	0,1% / 0,001%	
Comunicação	TCP/IP, RS-232, Wiegand	
	RS-485	
Temperatura / Umidade	-10~50 / Menos que 90%	
LCD	LCD gráfico de 128 x 64	
Tamanho	181 x 109 x 43 mm	
Adaptador AC/DC	Entrada: universal AC 100~250V	
	Saída: 12 VDC (Opcional: 24VDC)	
	Certificações UL, CSA, CE	
Opções	Leitor de Cartões RF	Cartão EM, 125kHz
	Leitor de Cartões SmartCard	Mifare Tipo A, 13,56MHz
	Interfone	

6. Informações durante operação do terminal

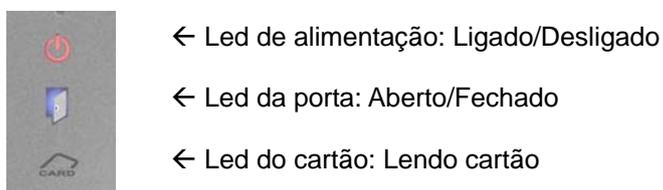
6.1 Descrição dos botões:

Para os visitantes apertarem esse botão para tocar a campainha do interfone

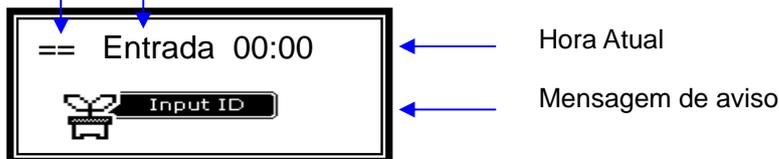
Para salvar as configurações quando estiver configurando o terminal.

6.2. Status do LED durante a operação

← Led de alimentação: Ligado/Desligado

← Led da porta: Aberto/Fechado

← Led do cartão: Lendo cartão

6.3. Mensagens na tela durante a operação

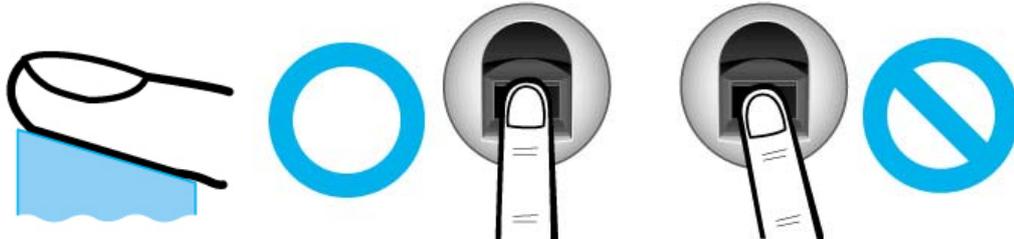
== Conectado ao servidor na rede
→← Desconectado do servidor na rede

Mostra: Entrada ou Saída quando está no Controle de Acesso (F1, F2, F3, F4)
Mostra: Entrada/Saída quando está em Controle de Ponto (Entrada, Saída, Descanso, Retorno, Normal)
Mostra o menu do Controle de refeição (MENU-1, MENU-2, MENU-3, MENU-4)

== 00:00 ViRDI 4000	- Tela Inicial
== 00:00 Input ID	- Insira o ID
== 00:00 Input FP	- Insira a digital
== 00:00 Password	- Digite a senha
== 00:00 Success	- Sucesso na autenticação
== 00:00 Matching fail	- Falha na autenticação
== 00:00 No record	- ID de usuário não cadastrado
== 00:00 Net error	- Quando o servidor não responde durante a tentativa de autenticação pelo servidor. - Caso o leitor seja desconectado do servidor durante a tentativa de autenticação pelo servidor

Tela	Descrição
→← 00:00 Connecting	- Quando há tentativa de conexão com o servidor e não há nenhum usuário cadastrado.
== 00:00 Place your card	- Aguardando a aproximação do cartão.
== 00:00 Time expired	- Caso seja feito uma tentativa de autenticação de usuário cadastrado, mas em um horário em que o acesso não seja permitido.
== 00:00 Verifying	- Aguardando resposta após fazer autenticação no servidor.
== 00:00 Locked	- O terminal está bloqueado. - Caso esteja no modo refeição e não esteja em algum horário de refeição.
== 00:00 Upgrading	- Fazendo upgrade no firmware do terminal (Não desligue o terminal enquanto estiver mostrando essa mensagem.)

7. Cadastro e posicionamento adequado do dedo

- Posicionamento adequado do dedo

  Se possível, use o dedo indicador e insira o dedo como se estivesse carimbando sua digital. Somente encostar o dedo no sensor não é suficiente para efetuar o cadastro.
  A forma adequada é encostar o centro da digital no sensor biométrico.

- Se possível use o dedo indicador.
  Usando o dedo indicador, pode-se obter uma impressão digital mais precisa e estável.

- Verifique se a digital está apagada ou se há cicatriz.
  Dedos muito secos ou molhados, com digital apagada ou com cicatriz são difíceis de serem reconhecidos. Nesses casos, use um dedo diferente para cadastro.

- Condições das digitais dos usuários

  A digital pode não ser reconhecida ou ser inconveniente seu uso, dependendo das suas condições.

  - Esse produto é um sistema de reconhecimento biométrico. Se a digital estiver danificada ou fraca, não pode ser usada. Nesse caso, use cartão RFID.
  - **Se a sua pele estiver muito seca, abafe sobre seu dedo para umedecê-lo.**

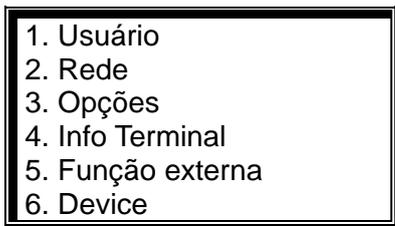
  - As digitais de crianças normalmente são muito pequenas ou são um pouco apagadas. É necessário recadastrar a digital a cada 6 meses.

  - As digitais de idosos podem ser difíceis de ser cadastradas por possuírem as linhas das digitais muito finas.
  - É recomendado o cadastro de pelo menos 2 digitais por pessoa.

8. Ambiente de configuração

8.1 - Entrar no Menu

Para entrar no Menu, aperte o botão [*] durante 2 segundos. A seguinte tela vai aparecer.

1. Usuário
2. Rede
3. Opções
4. Info Terminal
5. Função externa
6. Device

É necessária a autenticação do Administrador para fazer qualquer modificação na configuração do menu. Aparece a seguinte tela para autenticação do menu:

<Insira AdminID>
ID: 0001

Insira o ID do administrador e aperte [Enter]. Faça a autenticação de acordo com o que foi escolhido durante o cadastro (biometria/senha/cartão).
A autenticação do administrador é requerida somente uma vez e todos os sub menus ficam acessíveis até que saia do menu de configuração.

8.2. Mudar configurações

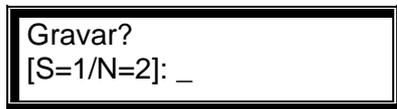
Para mudar as configurações, aperte [#] para apagar os valores antigos para inserir os novos valores.

Aperte [0] para aparecer o restante dos menus que não aparecem na tela do LCD, e aperte o número correspondente ao menu desejado.

Aperte [Enter] para entrar no menu desejado para verificar as configurações ou para ir para o menu seguinte. E aperte [#] para voltar para o menu anterior.

Aperte [#] durante 2 seg. para cancelar a configuração atual e para seguir para o próximo menu.

8.3. Salvando as modificações

Aperte [#] no menu principal para salvar as modificações realizadas e vai aparecer a seguinte tela:

Aperte [1] para salvar as mudanças, se não aperte [2]. Aperte Enter em seguida.

- Se não feito nenhuma mudança nas configurações, não vai aparecer nenhum menu para salvar.

- Durante a configuração, se não for digitado nem feito nenhuma ação durante um certo período de tempo, automaticamente vai sair do processo de configuração e voltar para a tela inicial. Se tiver sido feita alguma modificação nas configurações, vai aparecer a tela para Salvar. Se não, não aparece nada.

9. Descrição do Menu

Função		Detalhes
1. Usuário	1.Adicionar usuário	Cadastra um usuário para ter acesso a área onde o terminal está instalado
	2.Remover	Apaga um usuário cadastrado no terminal, digitando o ID do usuário a ser apagado.
	3.Modificar	Modifica o Nível 1:1, pode-se adicionar uma digital ou um cartão a um usuário já cadastrado.
	4.Adicionar Administrador	Cadastra um administrador para gerenciar o terminal.
	5.Remover tudo	Apaga todos os usuários e administradores.
2. Rede	1. Terminal ID	Atribuir um ID para o terminal.
	2. Endereço de IP	Configura um endereço de IP para o terminal.
	3. IP do Servidor	Configura o endereço de IP para o servidor de autenticação.
3. Opções	1. Aplicação	Configura o tipo de aplicação a ser usado no terminal: Controle de Acesso, Controle de Ponto ou Controle de refeição
	2. Opção de Verificação	Mostrar ou não ID ou nome do usuário ao fazer autenticação.
	3. Fechadura	Configura o tempo de abertura da fechadura.
	4. Configuração do Som	Configura o volume da voz, do beep e ativa ou desativa o alarme.
	6. Configuração do relógio	Ajusta o relógio e data no formato: aaaammddhhmmss (ano/mês/dia/hora/min/seg)
	6. Outras Config.	Ajusta a intensidade da luz de fundo do LCD.
4. Informação do Terminal		ID - Versão - Aplicação - Idioma - Modo verificação - Tipo de rede - End. Mac - End. IP - Gateway - Subnet mask - IP servidor - Porta servidor - Leitor de cartões - Formato do cartão – Sensor FP - Nível 1:1 - Nível 1:N - Máx user - Máx bio - Todos user - Todos admin – Todos biom. - 1:N user - todos biom - Todos Logs
5.Função externa	1. Bloquear Terminal	Bloqueia o terminal, não é possível fazer autenticação
	2. Ler No. Cartão	Lê o ID do cartão RFID
6. Dispositivo	1. Set Fn Key	Configura a tecla *
	2. Leitor de cartões	Configura o leitor de cartões
	3. Sensor biométrico	Configura o Nível 1:1, o nível 1:N e habilita I-Capture
	4. Wiegand	Ativa e configura a saída Wiegand e Site Code
	5. Conf. Sistema	Configura o número de caracteres do ID e o idioma
	6. Inicializar	Retorna as configurações para seus valores iniciais

9.1 Visão expandida do Menu

1.Usuário	1. Adicionar 2. Remover 3. Modificar 4. Adicionar Administrador 5. Remover tudo	
2.Rede	1. Terminal ID 2. Verificação:NS/SN/NO 3. Tipo de rede [IP fixo/DHCP] 4. Endereço de IP 5. Subnet Mask 6. Gateway 7. IP Servidor 8. Porta Servidor	
3.Opções	1. Aplicação	<Aplicação> 0. Controle de Acesso 1. Controle de Ponto 2. Controle de Refeição
		Caso a opção seja 0 ou 1: <Hora de entrada <Hora de saída <Hora de acesso
		2. Caso seja Controle de Refeição Café Almoço Jantar Ceia Lanche Sem limite
	2. Opção de verificação	Exibir ID Auto Enter Key Somente Cartão Habilitar 1:N Mostrar ID do Grupo Verity Multi-FP
	3. Fechadura	Tempo abertura Sensor da porta Alarme tempa aberta
	4. Config. Som	Volume da voz Volume do beep Conf. Alarme
	5. Config. relógio	
	6. Outras Config.	Luz de Fundo Display time
4.Info Terminal	T-ID = 0001 Ver = 10.41.00 Aplicação = Acesso Idioima = PT Verificação = SN Tipo de rede =Estático	

	End. Mac = 000265201111 End. IP = 192.168.0.3 Gateway = 192.168.0.1 Subnet Mask = 255.255.255.0 IP Servidor = 192.168.0.2 Porta Servidor = 2204 Leitor de Cartão = RF|SC|Wiegand Sensor biom = FOH01 Formato de Cartão = 0 Nível 1:1 = 4 Nível 1:N = 5 Máx User = 100 Máx FP = 100 Todos User = 0 Todos Admin = 0 Todos FP = 0 1:N User = 0 1:N FP = 0 Todos Log = 0	
5.Função externa	1. Bloquear terminal 2. Ler nº cartão.	
6.Dispositivo	1. Set Fn Key	Key On/Off
	2. Leitor de Cartão	Leitor de Cartões Formato de cartões
	3. Sensor Biom	Nível 1:1 Nível 1:N I-capture
	4. Wiegand	Saída Wiegand Site Code
	5. Config. Sistema	Tamanho ID Idioma
	6. Inicializar	1. Config Inicial 2. Apagar Log 3. Inic. Terminal

10. Configuração do Menu

Gerenciamento de Usuários

Cadastro de Usuário

Aperte [*] durante 2 segundos para entrar no Menu

Procedimento		
1. Usuário 2.Rede 3.Opções 4.Info Terminal	1. Adicionar 2. Remover 3. Modificar 4. Add Admin	**<User ID [NOVO]>** ID : _ _ _ _
Aperte [1] para gerenciamento de usuário	Aperte [1] para adicionar um novo usuário	Digite um ID para o novo usuário e aperte [Enter]
1. FP 2. ID&PW 3. FP|PW 4. FP&PW 5. RF 6. RF|FP 7. RF&FP 8. RF|PW	91. RF&PW | RF&FP 92. ID&FP | RF&FP 93. ID&PW | RF&PW	
Aperte [0] para mostrar para ver o restante do menu que não aparece na tela.	Selecione um modo. E digite o número correspondente ao modo desejado. Veja a descrição de cada autenticação na página 6.	

1. Cadastro escolhendo a opção: “1. FP” – Cadastro e autenticação por biometria

[*] → [1] → [1] → User ID [ENTER] → [1] → Nível 1:1 [ENTER] → Habilitar 1:N [ENTER] → Insira digital → Insira digital novamente

Valor recomendado: ‘0’

Pode ser designado um nível de segurança 1:1 diferente para cada usuário. Quando é colocado o valor “0”, a autenticação 1:1 usa o valor padrão configurado para o terminal em vez de usar um nível de autenticação diferente para cada usuário.
Quando é mudado o nível de autenticação 1:1 configurado para o terminal, é feito a mudança para todos os usuários que foram cadastrados com o valor ‘0’ de Nível 1:1

Aperte [ENTER] para seguir adiante.

<Habilitar 1:N>
(N=0/S=1): 0

Valor padrão é ‘0’, mas para habilitar a autenticação 1:N colocar ‘1’.

Caso não haja muitos usuários cadastrados ou para conveniência do usuário, pode-se fazer a autenticação do usuário inserindo a digital sem a necessidade de digitar o ID do usuário antes.
Para a autenticação sem a necessidade do ID, digite ‘1’.
Para a autenticação com a necessidade de digitar o ID, digite ‘0’.

Aperte [ENTER] para seguir adiante.

Vai soar um som de buzzer “ppiriririck” duas vezes, e em seguida vai acender a luz no sensor biométrico. Encoste a parte do dedo onde fica a impressão digital na superfície do sensor biométrico e aguarde de 2 a 3 segundos até que apague a luz do sensor e a digital seja salva.

É necessário fazer uma segunda leitura da digital para confirmação. Remova totalmente o dedo do sensor e encoste o dedo no sensor novamente.

Caso o cadastro ocorra com sucesso, vai soar um som “ppiririck”. E retorna para a tela “1. Adicionar”. Caso ocorra algum erro ou a imagem obtida não esteja com boa qualidade ou o sensor esperou mais que 10 seg. para obter uma resposta, é tocado um som de erro “pibig” e retorna para a tela “1.Adicionar”

Repita os processos acima 2 a 3 vezes para compreender o método correto para cadastro de usuários. Se ocorrer algum erro, é recomendado usar a senha para autenticação.

2. Cadastro escolhendo a opção: “2. ID&PW” – Cadastro e autenticação por Senha e ID

[*] → [1] → [1] → User ID [ENTER] → [2] → Digite a senha [ENTER] → Digite a senha novamente [ENTER]

Digite uma senha. A senha deve conter de 1 a 8 caracteres. Aperte [ENTER].

Digite a mesma senha para confirmação.

Caso o cadastro ocorreu com sucesso, vai tocar um som “piririck”, se não, vai tocar um som de erro “pibig” e volta para o menu “1.Adicionar”.

3. Cadastro escolhendo a opção: “3. FP|PW” – Cadastro e autenticação por biometria ou senha.

[*] → [1] → [1] → User ID [ENTER] → [3] → Digite senha [ENTER] → Digite a mesma senha [ENTER] → Nível 1:1 [ENTER] → Habilitar 1:N [ENTER] → Insira Digital → Insira a mesma digital

Para o cadastramento da digital, veja o procedimento “1.FP – Cadastro e autenticação por biometria” e em seguida, para cadastramento da senha, veja o procedimento “2. ID&PW – Cadastro e autenticação por Senha e ID”

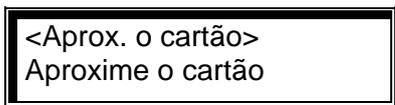
4. Cadastro escolhendo a opção “4. FP&PW” - Cadastro e autenticação por biometria e senha

[*] → [1] → [1] → User ID [ENTER] → [4] → Digite senha [ENTER]
→ Digite a mesma senha [ENTER] → Nível 1:1 [ENTER] → Habilitar 1:N [ENTER]
→ Insira Digital → Insira a mesma digital

Para o cadastramento da digital, veja o procedimento “1.FP – Cadastro e autenticação por biometria” e em seguida, para cadastramento da senha, veja o procedimento “2. ID&PW – Cadastro e autenticação por Senha e ID”

5. Cadastro escolhendo a opção “5. RF” - Cadastro e autenticação por cartão RFID.

[*] → [1] → [1] → User ID [ENTER] → [5] → Aproxime o Cartão

<Aprox. o cartão>
Aproxime o cartão

Para cancelar o cadastro, aperte [#] .

Aproxime o cartão RFID do terminal, vai tocar um som “piririck” caso o cadastro ocorreu com sucesso. Ou vai tocar um som de erro caso ocorreu algum erro. E retornará para a tela “1.Adicionar”.

6. Cadastro escolhendo a opção “6. RF|FP”- Cadastro e autenticação por Cartão ou biometria.

[*] → [1] → [1] → User ID [ENTER] → [6] → Aproxime o cartão → Nível 1:1 [ENTER] → Habilitar 1:N [ENTER] → Insira a digital → Insira a mesma digital

Para o cadastramento do cartão, veja o procedimento “5.FP – Cadastro e autenticação por cartão RFID” e em seguida, para cadastramento da biometria, veja o procedimento “1. FP” – Cadastro e autenticação por biometria

7. Cadastro escolhendo a opção “7. RF&FP” - Cadastro e autenticação por Cartão e biometria

[*] → [1] → [1] → User ID [ENTER] → [7] → Aprox. o cartão → Nível 1:1 [ENTER] → Habilitar 1:N [ENTER] → Insira a digital → Insira a mesma digital

Para o cadastramento do cartão, veja o procedimento “5.FP – Cadastro e autenticação por cartão RFID” e em seguida, para cadastramento da biometria, veja o procedimento “1. FP” – Cadastro e autenticação por biometria

8. Cadastro escolhendo a opção “8. RF|PW” - Cadastro e autenticação por Cartão ou Senha

[*] → [1] → [1] → User ID [ENTER] → [8] → Aprox. o cartão → Insira a digital [ENTER] → Insira a mesma digital [ENTER]

Para o cadastramento do cartão, veja o procedimento “5.FP – Cadastro e autenticação por cartão RFID” e em seguida, para cadastramento da biometria, veja o procedimento “2. ID&PW – Cadastro e autenticação por Senha e ID”

9. Cadastro escolhendo a opção “91. RF&PW” - Cadastro e autenticação por Cartão e Senha

[*] → [1] → [1] → User ID [ENTER] → [9][1] → Aprox. o cartão → Insira a senha [ENTER] → Digite a mesma senha [ENTER]

Para o cadastramento do cartão, veja o procedimento “5.FP – Cadastro e autenticação por cartão RFID” e em seguida, para cadastramento da biometria, veja o procedimento “2. ID&PW – Cadastro e autenticação por Senha e ID”

10. Cadastro escolhendo a opção “92. ID&FP|RF&FP” - Cadastro e autenticação por ID e biometria ou Cartão e biometria

[*] → [1] → [1] → User ID [ENTER] → [9][2] → Aprox. o cartão → Nível 1:1[ENTER] → Habilitar 1:N [ENTER] → Insira a digital→ Insira a mesma digital

Nesse caso, o cartão pode ser usado ao invés de digitar o ID para autenticação. É mais prático para usuários que têm dificuldade em digitar o ID.

Para o cadastramento do cartão, veja o procedimento “5.FP – Cadastro e autenticação por cartão RFID” e em seguida, para cadastramento da biometria, veja o procedimento “1. FP” – Cadastro e autenticação por biometria

11. Cadastro escolhendo a opção “93. ID&PW|RF&PW” - Cadastro e autenticação por ID e senha ou Cartão e senha.

[*] → [1] → [1] → User ID [ENTER] → [9][3] → Aproxime o cartão → Digite a senha [ENTER] → Digite a senha novamente [ENTER]

Nesse caso, o cartão pode ser usado ao invés de digitar o ID para autenticação. É mais prático para usuários que têm dificuldade em digitar o ID.

Para o cadastramento do cartão, veja o procedimento “5.FP – Cadastro e autenticação por cartão RFID” e em seguida, para cadastramento da biometria, veja o procedimento “2. ID&PW – Cadastro e autenticação por Senha e ID”

Remoção de Usuário

Aperte [*] durante 2 segundos para entrar no Menu

Procedimento		
1. Usuário 2.Rede 3.Opções 4.Info Terminal	1. Adicionar 2. Remover 3. Modificar 4. Add Admin 5. Remover tudo	**<User ID>** ID : _ _ _ _
Aperte * durante 2 segundos para entrar no Menu. Aperte [1] para gerenciamento de usuário	Aperte [2] para remover o usuário	Digite um ID do usuário a ser removido [Enter]

[*] → [1] → [2] → User ID [ENTER]

Todas as informações do usuário vão ser apagadas do terminal. Entretanto, as informações vão continuar no servidor até que seja completamente apagado do servidor.

Se for digitado um ID não cadastrado, o menu volta para a tela do “2. Remover” e é tocado um som de erro.

Atenção ao apagar um usuário ou administrador. Se o usuário foi recém cadastrado no terminal e não no servidor, o usuário não pode ser recuperado.

Remoção de Todos os Usuários

Aperte [*] durante 2 segundos para entrar no Menu

Procedimento		
1. Usuário 2.Rede 3.Opções 4.Info Terminal	5. Remover tudo	**Remover tudo?** [Y=1/N=2]: _
Aperte * durante 2 segundos para entrar no Menu. Aperte [1] para gerenciamento de usuário	Aperte [5] para remover todos os usuários	Para remover todos os usuários digite 1. Para cancelar digite 2. Todos os usuários e administradores vão ser apagados do terminal.

[*] → [1] → [5]

Cadastro de administrador

Aperte [*] durante 2 segundos para entrar no Menu

Procedimento		
1. Usuário 2.Rede 3.Opções 4.Info Terminal	1. Adicionar 2. Remover 3. Modificar 4. Add Admin	**<Admin ID [NOVO]>** ID : _ _ _ _
Aperte [1] para gerenciamento de usuário	Aperte [4] para adicionar um administrador	Digite um ID para o novo admin e aperte [Enter]
1. FP 2. ID&PW 3. FP|PW 4. FP&PW 5. RF 6. RF|FP 7. RF&FP 8. RF|PW	91. RF&PW | RF&FP 92. ID&FP | RF&FP 93. ID&PW | RF&PW	
Aperte [0] para mostrar para ver o restante do menu que não aparece na tela.	Selecione um modo. E digite o número correspondente ao modo desejado. Veja a descrição de cada autenticação na página 6.	

O cadastro do administrador segue os mesmos passos que o cadastramento de usuário. Veja os procedimentos em “Cadastro de usuário”.

Modificar um Usuário

Aperte [*] durante 2 segundos para entrar no Menu

Procedimento		
1. Usuário 2.Rede 3.Opções 4.Info Terminal	1. Adicionar 2. Remover 3. Modificar 4. Add Admin	**<User ID [MOD]>** ID : _ _ _ _
Aperte * durante 2 segundos para entrar no Menu. Aperte [1] para gerenciamento de usuário	Aperte [3] para modificar o usuário	Digite um ID do usuário a ser modificado [Enter]

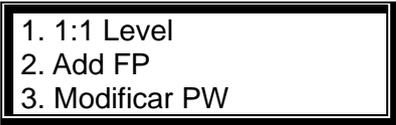
Se for digitado um ID não cadastrado, o menu volta para a tela do “1. Adicionar” e é tocado um som de erro.
Ao mudar um ID, não há diferença entre usuário e administrador.

1. Usuário “1. FP”

1. 1:1 Level 2. Add FP	Para mudar o nível segurança de autenticação, digite [1]. Para adicionar uma digital ao ID correspondente, digite [2]. Podem ser adicionadas no máximo 5 digitais para um mesmo ID.

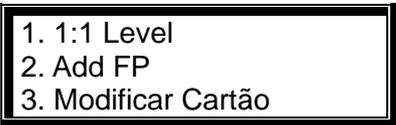
2. Usuário “2.ID&PW”

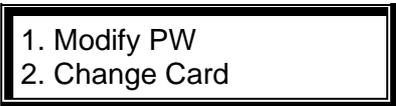
1. Modificar PW	Para modificar a senha digite [1], para cancelar aperte [#] . A senha deve conter de 1 a 8 dígitos. Para mudar a senha, digite a nova senha, aperte [ENTER] e digite novamente a nova senha e aperte [ENTER].

3. Usuário “3.FP|PW”, “4.FP&PW”

1. 1:1 Level 2. Add FP 3. Modificar PW	Aperte [0] para ver os menus escondidos. Para cancelar aperte [#] ou digite o número referente.

4. Usuário “5.RF”

1. Modificar Cartão	Para modificar o cartão RF cadastrado, aperte [1] e aproxime o novo cartão. Para cancelar aperte [#] .

5. Usuário “6.RF|FP”, “7.RF&FP”, “92.ID&FP|RF&FP”

1. 1:1 Level 2. Add FP 3. Modificar Cartão	Aperte [0] para ver os menus escondidos. Para cancelar aperte [#] ou digite o número referente.

6. Usuário “8.RF|PW”, “91.RF&PW”, “93.ID&PW|RF&PW”

1. Modify PW 2. Change Card	Para cancelar aperte [#] ou digite o número referente.

Configuração da Rede

Aperte [*] durante 2 segundos para entrar no Menu

Procedimento		
1. Usuário 2.Rede 3.Opções 4.Info Terminal	< Terminal ID > ID: 00000001	Modo [NS / SN / NO] (0-2): 0
Entre no menu e aperte [2] para configurar a Rede'	Esse ID é único para cada terminal para ser distinguido pelo servidor. Deve ser o mesmo que o ID da porta configurado no servidor. Aperte [Enter].	Para selecionar o Modo NS digite '0', SN digite '1' , NO digite '2'. [Enter]

Modos de autenticação:

NS	Com o servidor conectado, a autenticação é feita pelo servidor. Somente se estiver desconectado devido a algum erro na rede, a autenticação é feita pelo terminal.
SN	Mesmo com o servidor conectado, é feito a busca da autenticação na memória do terminal e o resultado é mandado para o servidor em tempo real. Mas se o usuário não estiver cadastrado no terminal, a busca é feita na memória do servidor, para autenticação 1:1. (Caso seja feita autenticação 1:N, não é feito a busca no servidor).
NO	Mesmo que o usuário esteja cadastrado no terminal, a autenticação somente é feita pelo servidor. Se o servidor estiver desconectado, não vai ser possível fazer nenhuma autenticação.

Dependendo do número de terminais e de usuários ou das condições da rede, cada modo pode ser usado flexivelmente. Mas se tiver mais que dez terminais conectados ao servidor para autenticação simultânea, ou se houver problemas freqüentes na rede, é recomendado usar a autenticação SN.

Network Type:0 0:Static 1:DHCP	<End. IP> 192.168.0.3	<Subnet Mask> 255.255.255.0
Digite [0] para IP fixo e [1] para DHCP. [Enter]	Aperte [#] para apagar. Digite o End. de IP. [ENTER]	Aperte [#] para apagar. Digite o Subnet Mask [Enter].

<Gateway> 192.168.0.1	<IP Servidor > 192.168.0.2	< Porta Servidor > Num: 2201
Aperte [#] para apagar. Digitar o Gateway.	Aperte [#] para apagar o valor antigo e digite o novo valor. Aperte [Enter]	Aperte [#] para apagar o valor antigo e digite o novo valor. Aperte [Enter]

Seleção de Opção do Sistema

Configurando aplicação

Aperte [*] durante 2 segundos para entrar no Menu

Procedimento		
1. Usuário 2.Rede 3.Opções 4.Info Terminal	1. Aplicações 2. Verify Option	Aplicação: 0 0= Ctrl Acesso 1= Ctrl Ponto 2= Ctrl Refeição
Entre no menu e aperte [3] para configurar as opções	Para configurar o modo de aplicação do terminal, digite [1].	O valor padrão é ‘0’. Aperte [Enter].

Na aplicação **Controle de Acesso** não há nenhuma outra configuração a mais.

No menu <Aplicação> caso seja selecionado a opção ‘**1. Ctrl de Ponto**’ aparecem os menus para configurar o intervalo para o horário de entrada, saída, descanso e retorno.
Após a autenticação, o modo que aparece no display pode ser automaticamente mudado para o modo de operação programado. Se <multi-key authentication> for configurado como o modo de operação, podem ser definidos mais de 40 modos.

Hora de Entrada é o horário de entrada para início do trabalho. Insira o intervalo de horário para o terminal poder ser acessado para a entrada. Caso não seja necessário definir o intervalo para entrada, coloque ‘00:00-00:00’.
A menos que algum botão de função seja apertado, o modo de operação (Entrada[F1]/Saída[F2]) sempre vai aparecer na tela de acordo com o horário ajustado.
Após configurar o horário de entrada, configure o horário de saída. O horário de entrada não deve sobrepor o de saída.

Depois de configurar a “Hora de Acesso”, aparece o menu <Multi Fn-Key> que permite mais de 5 modos de operação:

```
<Multi Fn-key>
1=F1: X  2=F2: X
3=F3: X  4=F4: X
```

Valor padrão: tudo ‘X’

Esse menu é útil quando mais de 5 modos de operação são necessários.
- Configuração X: cada tecla de função representa um modo de operação, como F1=Início, F2=Saída, F3=Descanso e F4=Retorno. Quando a tecla de função é apertada, o modo de autenticação muda de acordo com o modo de operação correspondente.
- Configuração 0: o modo é definido pela combinação da tecla de função e um número, como “F3+1”.
Ex.: Se a configuração for: 1=F1:X, 2=F2:X, 3=F3:X, 4=F4: 0. Podem ser definidos 14 modos diferentes de operação de acordo com a combinação do [F4]+’0’ até [F4]+’9’.
Aperte [Enter] para salvar.

No menu <Aplicação> caso seja selecionado a opção **‘2. Ctrl de Refeição’**, insira o intervalo de horário para Café da manhã, Almoço, Jantar, Ceia e Lanche. Cada um dos horário não deve sobrepor o outro. Caso não seja usada alguma das refeições, coloque 00:00~00:00 no intervalo. Caso tenha algum intervalo de horário que não tenha sido usado para nenhuma das refeições, vai aparecer a mensagem: “Bloqueado!” na tela do terminal.

É possível fazer uma autenticação por usuário em cada período, mas se for necessário fazer uma segunda refeição no mesmo período, faça a autenticação da digital ou cartão enquanto aperta-se a tecla [ENTER].

Aperte [ENTER] após terminar de realizar todas as configurações.

Configurando opção de verificação

Aperte [*] durante 2 segundos para entrar no Menu

1.Usuário 2. Rede 3. Opções 4.Info Terminal	1. Aplicação 2. Verify Option 3. Fechadura 4. Config. do som	<Exibir ID> (0=Não / 1= Sim)
Entre no menu e aperte [3] para configurar as opções	Para configurar o método de autenticação aperte [2].	Deseja mostrar ou não ID do usuário quando for feito a autenticação. Ex: OK! <0001> Se não aparece somente a mensagem: OK! Aperte [ENTER].
<Auto Enter Key> (N=0/S=1):0	<Somente Cartão> (N=0/S=1): 0	<Habilitar 1:N> (N=0/S=1): 1
Para habilitar a função digite 1 ou para desabilitar digite 0. Aperte [ENTER] em seguida.	Para habilitar a função digite 1 ou para desabilitar digite 0. Aperte [ENTER] em seguida.	Para habilitar a função digite 1 ou para desabilitar digite 0. Aperte [ENTER] em seguida.

Função Auto Enter Key

Se estiver desabiliado, o usuário tem que digitar o ID e apertar [F1]~[F4] antes de fazer a autenticação para escolher o tipo de operação. Se habilitado, não é necessário digitar a tecla de função.

Função somente Cartão

Se a função estiver habilitada, o usuário somente precisa apresentar o cartão para autenticação. Mesmo que o modo de autenticação do usuário seja por RF&PW ou RF&FP.
Essa opção é normalmente usada quando há muitos terminais instalados e há muitas pessoas entrando e saindo e quando o nível de segurança for relativamente baixo.

Função Habilitar 1:N

Se habilitado, essa função permite autenticação do usuário por biometria sem que seja necessário digitar o ID do usuário ou apresentar o cartão. Mesmo que o usuário esteja cadastrado para ser autenticado por autenticação 1:N, somente a autenticação 1:1 vai ser permitida se o valor estiver '0'.

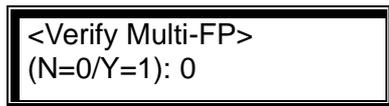
Se a Autenticação 1:N for habilitada (valor '1'), aparece a função <User ID Group>

<User ID Group> (N=0/S=1): 0	Valor padrão: '0'

Os primeiros dígitos do ID são tratados como um grupo para autenticação. Então a autenticação 1:N pode ficar mais rápida quando tiver mais que 1.000 pessoas cadastradas.

Se essa função estiver habilitada (valor '1') a autenticação por biometria é comparada com usuários cujos primeiros dígitos de ID são iguais ao ID digitado.
Se essa função estiver desabilitada (valor '0') o número digitado é tratado como o ID do usuário e é feita a comparação 1:1 da biometria com o ID digitado.

Ex.) O ID do usuário possui 4 dígitos, e é digitado '12' para autenticação. Se a autenticação 1:N estiver Habilitada, então é feito a comparação com os IDs de 1200 a 1299. Se não estiver habilitada, a autenticação é comparada com a digital do usuário de ID 12.

Se a Autenticação 1:N não for habilitada (valor '0'), aparece a função <Verify Multi-FP>

Default setting: '0'

Para fazer a autenticação, é necessário que todos os usuários digitem o ID (ou apresentar o cartão).

Essa função normalmente é usada para controlar áreas que requerem maior segurança no acesso. Se o usuário de ID0001 possuir 3 digitais cadastradas no terminal, então ele tem que digitar o ID e fazer a autenticação de todas as 3 digitais.

A seqüência de autenticação das 3 digitais não faz diferença, mas se uma das três digitais não for reconhecida, vai ocorrer erro na autenticação.

Configurando a fechadura

Aperte [*] durante 2 segundos para entrar no Menu

1.Usuário 2. Rede 3. Opções 4.Info Terminal	1. Aplicação 2. Verify Option 3. Fechadura 4. Config. do som	<Tempo Abertura> (00-30):03
Entre no menu e aperte [3] para configurar as opções.	Para configurar a fechadura aperte [3].	Configurar o tempo de abertura da porta. Se for colocado '00', a porta não está sendo controlada. Aperte [ENTER].
<Sensor da Porta > [0/1=NA/2=NF]: 0		Alarme de porta aberta (00-30):00
0. Sem monitoração 1. Fechadura do tipo Dead bolt ou porta automática (Monitoramento da porta é ativado quando a porta estiver fechada) 2. Fechadura tipo Strike (monitoramento é desligado quando a porta está fechada). Aperte [ENTER]		O terminal verifica quanto tempo a porta está aberta. Caso exceda o limite estabelecido, soa um alarme. (Min 05 ~ Máx. 30seg) Se for colocado '00' o alarme é desativado.

Para usar essa função, a fechadura tem que ter uma função de monitoração que verifique o estado da porta aberta/fechada. E também a Função de verificação de porta aberta ('Sensor da porta') no item anterior tem que estar setado para '1' ou '2', para que essa função funcione.

Configurando o volume do som

Aperte [*] durante 2 segundos para entrar no Menu

1.Usuário 2. Rede 3. Opções 4.Info Terminal	1. Aplicação 2. Verify Option 3. Fechadura 4. Config. do som	<Habilitar Voz> (N=0/S=1): 1
Entre no menu e aperte [3] para configurar as opções.	Para ajustar o volume aperte [4].	Valor padrão '1'. Habilita ou não as mensagens de voz. Aperte [ENTER].
<Volume Beep> (0-2): 1	<Config. Alarm> (N=0/S=1): 0	
Valor padrão '1' Ajuste do volume do beep. '0' sem som, '1' volume baixo e '2' volume alto. Aperte [ENTER]	Soar ou não alarme contra violação da tampa. Valor padrão 'Sim' Aperte [ENTER].	

Configurando Hora e Data

Aperte [*] durante 2 segundos para entrar no Menu

1.Usuário 2. Rede 3. Opções 4.Info Terminal	1. Aplicação 2. Verify Option 3. Fechadura 4. Config. do som 5. Config. Relógio 6. Outras config.	<Config. Hora> 20100118121035
Entre no menu e aperte [3] para configurar as opções.	Para ajustar o relógio e data aperte [5].	Formato: ano/mês/dia/hora/min/seg aaaa/mm/dd/hh/mm/ss Ex. 2010: ano, 01: Mês, 18: Dia, 12: hora, 10: Minuto, 35:Segundo Para modificar aperte [#] e digite o valor correto. Aperte [ENTER] para salvar.

Configurando a luz do LCD e formato da hora

Aperte [*] durante 2 segundos para entrar no Menu

1.Usuário 2. Rede 3. Opções 4.Info Terminal	1. Aplicação 2. Verify Option 3. Fechadura 4. Config. do som 5. Config. Relógio 6. Outras config.	<Luz de Fundo> (0=deslig/1=ligado): 0
Entre no menu e aperte [3] para configurar as opções.	Para ajustar outras configurações aperte [6].	Caso seja selecionado ''1. Ligado' a luz do LCD vai permanecer sempre ligada. Caso seja selecionado '2. Desligado' a luz do LCD é ligada quando estiver em operação somente. Aperte [ENTER]
<Display time > 0=24h 1=AM/PM	Sensor monitor: 0 0=Desligado 1= Fire sensor 2= Sensor monitor	
Formato da hora para aparecer no LCD. Aperte [ENTER]	Selecione uma opção e aperte [Enter]	

Informações sobre o Terminal

Aperte [*] durante 2 segundos para entrar no Menu. Entre no menu e aperte [4] para ver as informações sobre o terminal.

Descrição dos itens da Informação do Terminal:

T-ID	ID do Terminal
Ver	Versão do Firmware do terminal
Aplicação	Modo de operação do Terminal
Idioma	Idioma selecionado
Modo verific.	Forma de autenticação
Tipo da rede	Tipo da rede escolhida (IP fixo/IP dinâmico)
Mac-Address	Endereço físico da placa de rede do terminal
End. IP	Endereço de IP do terminal
Gateway	Endereço do Gateway do terminal
Subnet Mask	Endereço do Subnet Mask do terminal
IP Servidor	Endereço do IP do Servidor conectado ao terminal
Porta Servidor	Número da porta do servidor
Leitor Cartões	Tipo de Leitor de cartões (RF|SC|Wiegand ou SmartCard)
Sensor biom.	Tipo do sensor biométrico
Formato Cartão	Tipo de formato dos dados do cartão
Nível 1:1	Nível de segurança usado para autenticação 1:1
Nível 1:N	Nível de segurança usado para autenticação 1:N
Máx user	Capacidade máxima de usuários
Máx FP	Capacidade máxima de templates
Todos User	Quantidade de usuários e administradores cadastrados no terminal
Todos Admin	Quantidade de administradores cadastrados no terminal
Todos biom	Quantidade de digitais cadastradas no terminal
1:N User	Quantidade de usuários cadastrados como 1:N
1:N biom	Quantidade de digitais cadastradas como 1:N
Todos Logs	Quantidade de logs registrados

Função externa

Bloqueio do terminal

Aperte [*] durante 2 segundos para entrar no Menu

Procedimento		
1.Usuário 2. Rede 3. Opções 4.Info Terminal 5. Função externa 6. Dispositivo	1. Bloquear terminal 2. Ler No. do cartão	<Bloquear terminal?> (N=0/S=1): 0
Entre no menu e aperte [5] para entrar em Função externa.	Para bloquear o terminal aperte [1].	Quando o terminal é bloqueado, ninguém pode fazer acesso ao terminal nem à porta. Escolha uma opção e digite [ENTER].
Para permitir acesso ao administrador o item “Permitir acesso ao administrador” deve estar checado, no servidor. Aperte [F4] para salvar.		

Ler número do cartão

Aperte [*] durante 2 segundos para entrar no Menu

1.Usuário 2. Rede 3. Opções 4.Info Terminal 5. Função externa 6. Dispositivo	1. Bloquear terminal 2. Ler No. do cartão	<Aprox. o Cartão>
Entre no menu e aperte [5] para entrar em Função externa.	O terminal com leitor de cartão tem uma função para ler o número do cartão para que possa ser cadastrado no servidor. Aperte [2].	Aproxime o cartão e o número é mostrado automaticamente na tela. Aperte [#] para sair.

Configuração do Dispositivo

Aperte [*] durante 2 segundos para entrar no Menu. E aperte [6] para entrar em 6.Dipositivo. **A senha para entrar nesse menu é: ‘ 0 8 4 2 6 5 ’**

Procedimento		
1.Usuário 2. Rede 3. Opções 4.Info Terminal 5. Função externa 6. Dispositivo	<Insira PW> PW:	1. Config Fn Key 2. Leitor Cartões 3. Sensor Biom. 4. Wiegand 5. Config. Sistema 6. Inicializar
Entre no menu e aperte [6] para entrar em Device.	Digite ‘ 0 8 4 2 6 5 ’ E aperte [ENTER]. Essa senha não pode ser mudada.	Veja abaixo cada item detalhado.

Configuração do Sistema: ID e Idioma

Aperte [*] durante 2 segundos para entrar no Menu. E aperte [6] para entrar em 6.Dipositivo. **A senha para entrar nesse menu é: ‘ 0 8 4 2 6 5 ’**

[*] → [6] → “084265” [ENTER] → [5] → [ENTER]

1. Config Fn Key 2. Leitor Cartões 3. Sensor Biom. 4. Wiegand 5. Config. Sistema 6. Inicializar	<Tamanho ID> (2-8): 4	<Idioma>:4 0=KOR 1=ENG 2=JPN 3=ESP 4=POR 5=CHN
Digite [5] para entrar em configuração do sistema.	O tamanho do ID deve ser o mesmo que está cadastrado no servidor. Se tiver um ID cadastrado como ‘000075’, digite 6. Aperte [ENTER].	Digite 4 para selecionar idioma Português Aperte [ENTER].

Configuração das teclas de função

Aperte [*] durante 2 segundos para entrar no Menu. E aperte [6] para entrar em 6.Dipositivo. **A senha para entrar nesse menu é: ‘ 0 8 4 2 6 5 ’**

[*] → [6] → ‘084265’ [ENTER] → [1]

1. Config Fn Key 2. Leitor Cartões 3. Sensor Biom. 4. Wiegand 5. Config. Sistema 6. Inicializar	<Key On/Off> 1=F1:O 2=F2:O 3=F3:O 4=F4:O 5=Ent:O 6=FP:O	
Digite [1] para entrar em configuração da teclas de função.	Escolher quais teclas de função vão ser habilitadas ou não.'0' habilita e 'X' desabilita. Aperte o número correspondente para mudar entre 0/X. Aperte [ENTER] para salvar.	

1 para [F1], 2 para [F2], 3 para [F3], 4 para [F4], 5 para [ENTER], e 6 para a auto-detecção do sensor biométrico.
Se apertar [1], o F1 muda para '0', e então o modo F1 fica desabilitado, ou seja, não pode-se mudar para o modo Entrada mesmo se apertar a tecla [F1] na autenticação.
Também se [F1] ou [F2] forem mudados para '0', o terminal pode ser usado somente para Entrada ou somente para saída. (F1 = Entrada / F2 = Saída)

Configurando o leitor de cartões

Aperte [*] durante 2 segundos para entrar no Menu. E aperte [6] para entrar em 6.Dipositivo. **A senha para entrar nesse menu é: ' 0 8 4 2 6 5 '**

[*] → [6] → '084265' [ENTER] → [2]

1. Config Fn Key 2. Leitor Cartões 3. Sensor Biom. 4. Wiegand 5. Config. Sistema 6. Inicializar	Leitor de Cartões: 0 0=Non 1=RF 2=SC 3=Wiegand 4=SC1 5=Ext 6=FP Card	<Card Format>: 0 0= Hex 8byte 1= Hex 16byte 2= Decimal
Digite [2] para entrar nas configurações do leitor de cartões.	Selecione o tipo de leitor do cartão de acordo com o instalado. 0 = sem leitor 1 = Leitor de cartão de 125kHz instalado 2 = Leitor de cartão Mifare instalado 3 = Leitor de cartão tipo Wiegand 4 = Nova versão de leitor instalado 5 = Leitor externo instalado 6 = Template no cartão Se essa função estiver configurada com um valor que não seja '0' e for apertado [F1]~[F4] ou [ENTER] somente o modo de autenticação é mudado e a autenticação 1:N não é realizada. Entretanto, a autenticação 1:N é realizada somente para auto-detecção. Aperte [ENTER] para salvar.	

Configurando o nível de segurança do sensor biométrico

Aperte [*] durante 2 segundos para entrar no Menu. E aperte [6] para entrar em 6.Dipositivo. **A senha para entrar nesse menu é: ' 0 8 4 2 6 5 '**

[*] → [6] → '084265' [ENTER] → [3]

1. Config Fn Key 2. Leitor Cartões 3. Sensor Biom. 4. Wiegand 5. Config. Sistema 6. Inicializar	<Nível 1:1> (1-9): 4	<Nível 1:N> (3-9): 5
Digite [3] para entrar nas configurações do sensor biométrico.	Valor padrão '4' Selecione o nível de autenticação. Quanto maior o número maior a segurança. Contudo, a taxa de rejeição aumenta. Aperte [ENTER] para continuar.	Valor padrão '5' Selecione o nível de autenticação. A comparação é feita dentre as templates que permitem autenticação 1:N. Aperte [ENTER] para continuar.

Autenticação 1:1 é quando o usuário tem que digitar um ID e sua digital é comparada somente com a digital cadastrada no ID digitado. Não é feito a comparação com todas as digitais cadastradas.
Autenticação 1:N é quando a digital inserida é comparada com todas as digitais cadastradas que permitem autenticação 1:N

Função de prevenção contra imitação de digital: LFD (Detecção de dedo falso)

<LFD> (0-3): 0

Valor padrão 0 (Muito baixo).

1 - Baixo: Prevenção contra imitação de digitais feitas de borracha e silicone.
2- Médio: Prevenção contra imitação de digitais feitas de borracha, silicone e certos tipos de papel e filme (objetos secos).
3- Alto: Prevenção contra imitação de digitais feitas de borracha, silicone, gelatina e certos tipos de papel e filme (objetos molhados).

Aperte Enter para salvar.

Configurar a saída Wiegand

Aperte [*] durante 2 segundos para entrar no Menu. E aperte [6] para entrar em 6.Dipositivo. **A senha para entrar nesse menu é: ‘ 0 8 4 2 6 5 ’**

[*] → [6] → “084265” [ENTER] → [4]

1. Config Fn Key 2. Leitor Cartões 3. Sensor Biom. 4. Wiegand 5. Config. Sistema 6. Inicializar	Wiegand Out: 0 0=None 1=26bit 2=34bit	<Site Code> (0-255): 000	<Bypass> (0=OFF / 1=ON) : 0
Digite [4] para entrar nas configurações da saída Wiegand.	Escolha uma opção e aperte [ENTER] para salvar.	Essa função é usada quando deseja-se conectar um controlador adicional pela conexão Wiegand. Aperte [ENTER] para salvar.	0=Desligado 1=Ligado

Configuração da Saída Wiegand:

0. Sem	Selecione essa opção caso não seja usado a saída Wiegand.
1. 26bit	É mandado: “Sitecode [1byte] + ID do usuário [2bytes] ” o ID do usuário deve possuir menos que 4 dígitos.
2. 34bit	É mandado: “Sitecode [1byte] + ID do usuário [3bytes]” o ID do usuário deve possuir menos que 7 dígitos.

Inicialização

Aperte [*] durante 2 segundos para entrar no Menu. E aperte [6] para entrar em 6.Dipositivo. **A senha para entrar nesse menu é: ' 0 8 4 2 6 5 '**

Apagando as configurações modificadas.

[*] → [6] → "084265" [ENTER] → [6] → [1]

1. Config Fn Key 2. Leitor Cartões 3. Sensor Biom. 4. Wiegand 5. Config. Sistema 6. Inicializar	1. Init Config 2. Apagar Log 3. Init Terminal	<Init Config> [S=1 / N=2]: 2
Digite [6] para entrar em Inicializar.	Aperte [1] para apagar todas as configurações. Exceto o Endereço Mac, usuários e registros de log não são apagados.	Digite '1' para apagar as configurações ou '2' para cancelar. Aperte [ENTER].

Apagando registros de evento

Aperte [*] durante 2 segundos para entrar no Menu. E aperte [6] para entrar em 6.Dipositivo. **A senha para entrar nesse menu é: ' 0 8 4 2 6 5 '**

[*] → [6] → "084265" [ENTER] → [6] → [2]

1. Config Fn Key 2. Leitor Cartões 3. Sensor Biom. 4. Wiegand 5. Config. Sistema 6. Inicializar	1. Init Config 2. Apagar Log 3. Init Terminal	<Apagar todos Logs> [S=1 / N=2]: 2
Digite [6] para entrar em Inicializar.	Aperte [2] para apagar todos os registros de log. Configurações e usuários não são apagados.	Digite '1' para apagar os logs ou '2' para cancelar. Aperte [ENTER].

Resetar o terminal

Aperte [*] durante 2 segundos para entrar no Menu. E aperte [6] para entrar em 6.Dipositivo. **A senha para entrar nesse menu é: ' 0 8 4 2 6 5 '**

[*] → [6] → "084265" [ENTER] → [6] → [3]

1. Config Fn Key 2. Leitor Cartões 3. Sensor Biom. 4. Wiegand 5. Config. Sistema 6. Inicializar	1. Init Config 2. Apagar Log 3. Init Terminal	<Init Terminal> [S=1 / N=2]: 2
Digite [6] para entrar em Inicializar.	Aperte [3] para resetar o terminal. Todos os usuários, administradores, log e configurações são apagados.	**Atenção! Todos os usuários, administradores, log e configurações são apagados.** **Aperte '1' para confirmar ou '2' para cancelar.**

12. Como usar o terminal

1 - Autenticação para Controle de Acesso

Modo normal, autenticação usando [ENTER]

Modo F1; autenticação usando [F1]

Modo F2; autenticação usando [F2]

Modo F3; autenticação usando [F3]

Modo F4; autenticação usando [F4]

Na aplicação para Controle de Acesso, o processo de autenticação normalmente é feito no modo Normal, apertando o botão [ENTER] ou apenas usando a auto-detecção do sensor biométrico, sem a necessidade de apertar nenhuma tecla de função.
Para uma operação mais detalhada para a aplicação de controle de acesso, o administrador pode especificar as funções para F1, F2, F3 e F4 de acordo com as necessidades. Esses modos não são especificados pelo fabricante.

- Autenticação biométrica
Aperte a tecla de função para o modo correspondente de autenticação.
Se a tecla de função não é usada e a autenticação é feita usando AutoDetecção,então vai ser usado o modo de autenticação atual que aparece na tela.

- Autenticação com password
Digite primeiramente o ID e mude o modo de autenticação apertando a tecla de função correspondente. Digite então a senha.

- Autenticação por cartão
Apertar a tecla de função correspondente ao modo de autenticação para inserir o cartão.

1.1– Autenticação por biometria 1:1

- Quando a auto-detecção estiver ativada, digite o ID (Ex. '0001') e então insira a digital no sensor. A luz do sensor acende e detecta a digital. O resultado da autenticação é mostrado na tela.
- Se for digitado o ID e o usuário apertar uma tecla de função, a luz no sensor acende junto com a mensagem de voz. Insira a digital e o resultado da autenticação é mostrado na tela.

1.2– Autenticação por biometria 1:N

Essa autenticação é permitida somente para usuários que estão habilitados para autenticação 1:N.

- Encoste o dedo no sensor biométrico e o sensor vai auto-detectar a digital. O resultado da autenticação é mostrado na tela.

- Na tela inicial, aperte uma tecla de função. A luz no sensor biométrico vai acender junto com a mensagem de voz. Insira a digital e o resultado da autenticação é mostrado na tela.

- Caso o usuário esteja cadastrado com biometria e senha, é necessário digitar a senha após a autenticação da digital.

1.3 – Autenticação por senha

- Digite o ID do usuário e aperte uma tecla de função. Digite a senha corretamente e aperte [ENTER]. O resultado da autenticação é mostrado na tela.

1.4 – Autenticação por cartão

- Caso o usuário esteja cadastrado como [RF], [RF|FP] ou [RF|PW], aproxime o cartão do terminal. O resultado é mostrado na tela.

- Caso o usuário esteja cadastrado como [RF&FP] ou [ID&FP|RF&FP], aproxime o cartão do terminal. Aguarde o resultado da autenticação, e quando aparecer a mensagem "Insira sua digital" insira a digital no sensor biométrico. O resultado da autenticação é mostrado na tela.

- Caso o usuário esteja cadastrado como [RF&PW] ou [ID&PW|RF&PW], aproxime o cartão do terminal. Aguarde o resultado da autenticação e quando aparecer a mensagem "Password" digite a senha e aperte [ENTER].

1.5 – Autenticação usando Grupo de ID.

A autenticação é feita digitando os primeiros dígitos (pelo menos um dígito) do ID em vez de digitar todo o ID. É mais conveniente do que a autenticação 1:1.
Essa autenticação é usada quando há muitos usuários cadastrados e então a autenticação 1:N não pode ser usada, ou quando o tempo de autenticação 1:N está muito lento.
Para configurar essa opção de autenticação, entre no menu, seguindo os passos:
* → 3. Opções → 2. Opção de verificação → ... → <Habilitar 1:N> = 1 → <User ID Group> = 1
Digite os primeiros dígitos do ID (se o ID for '1234' digite somente '12'), e então insira a digital. A digital vai ser comparada apenas com as digitais dos IDs de 1200 a 1299.

1.6 – Autenticação usando Várias digitais

- Para uma porta que necessita de alto nível de segurança, várias digitais de mais que duas pessoas podem ser designadas ao mesmo ID. A porta somente vai abrir se todas as digitais cadastradas forem autenticadas.
Para configurar essa opção de autenticação, entre no menu, seguindo os passos:
* → 3. Opções → 2. Opção de verificação → ... → <Habilitar 1:N> = 0 → <Verify Multi-FP> = 1

- Digite o ID e aperte uma tecla de função. A luz no sensor biométrico vai acender junto com a mensagem de voz. Insira a digital e o resultado da autenticação é mostrado na tela.